UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MATT GROVE, individually and on behalf of all others similarly situated, Plaintiff, v. COINBASE, INC. and COINBASE GLOBAL, INC., Defendants.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Matt Grove, individually and on behalf of the Class defined below of similarly situated persons ("Plaintiff and Class Members"), alleges the following against Defendants Coinbase, Inc. and Coinbase Global, Inc. (together, "Coinbase" or "Defendants"). The following allegations are based on Plaintiff's knowledge, investigations by Plaintiff's counsel, facts of public record, and information and belief:

NATURE OF THE ACTION

1. Plaintiff brings this action against Coinbase because of its failure to properly secure and safeguard highly valuable, protected, personally identifiable information including, *inter alia*, names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance records and transaction history), and limited corporate data (including documents, training material, and communications available to support agents) (collectively, "PII"); and for its failure to comply with industry standards to protect

information systems that contain PII.[1]

2. Coinbase is a cryptocurrency exchange with a quarterly trading volume of $393 billion. Coinbase says that it "is on a mission to increase economic freedom for more than 1 billion people."[2]

3. In order to obtain Defendants' services, Coinbase's customers have to directly or indirectly entrust Coinbase with their PII, which Coinbase uses in order to perform its regular business services.

4. As a cryptocurrency exchange, Coinbase therefore knowingly collects and stores sensitive PII of its customers, and has a resulting duty to secure such information from unauthorized access and exfiltration.

5. Coinbase expressly recognizes these duties, representing that "We at Coinbase … respect and protect the privacy of those who explore our Services ("**Users**") and Users who sign up for and access our Services ("**Customers**")."[3]

6. Despite its duty to safeguard individuals' PII, on May 11, 2025, Coinbase became aware of a cybersecurity incident as Coinbase received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer- service and account-management systems. The communication demanded ransom in exchange for not publicly

---

[1] Form 8-K, Coinbase Global, Inc. (May 14, 2025), located at https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc. (last accessed on May 30, 2025).

[2] *About Coinbase*, COINBASE, located at https://www.coinbase.com/about (last accessed on May 30, 2025).

[3] *Coinbase Global Privacy Policy*, COINBASE (last updated March 26, 2024), located at https://www.coinbase.com/legal/privacy (last accessed on May 30, 2025).

disclosing the information. The threat actor appears to have obtained this information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems (the "Data Breach" or "Breach").[4]

7. As a direct and proximate result of Coinbase's negligent failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII—names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents)—is now in the hands of cybercriminals.

8. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiff brings claims for negligence, negligence *per se*, unjust enrichment, and declaratory judgment, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in Defendants' possession in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

10. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and

[4] Form 8-K, *supra* note 1.

the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff (and many members of the Class) are citizens of states different than Defendants.

11. This Court has general personal jurisdiction over Defendants because Defendants' principal place of business and headquarters are in New York, NY. Defendants also regularly conduct substantial business in New York.

12. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conduct substantial business in this District.

PARTIES

13. Plaintiff Matt Grove, at all relevant times, is and was a citizen of the State of California. Plaintiff has used Defendants' cryptocurrency exchange since 2020.

14. Defendant Coinbase, Inc. is a Delaware corporation with a principal place of business located at One Madison Avenue, Suite 2400, New York, New York 10016.

15. Defendant Coinbase Global, Inc. is a Delaware corporation with a principal place of business located at One Madison Avenue, Suite 2400, New York, New York 10016.

CLASS ACTION ALLEGATIONS

16. Plaintiff, individually and on behalf of all others similarly situated, brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the Coinbase Data Breach (the "Class").

17. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors, and members of their officers' and directors' immediate families, any entity in

which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of those judicial officers' immediate families.

18. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

19. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including, but not limited to, the files implicated in the Data Breach. Upon information and belief, the Class, at a minimum, comprises over one million individuals.[5]

20. **Commonality.** This action involves questions of law and fact that are common to Plaintiff and the Class Members. Such common questions include, but are not limited to:

- Whether and to what extend Defendants had a duty to protect the PII of Plaintiff and Class Members;
- Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII;
- Whether Defendants had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

[5] Sergiu Gatlan, *Coinbase data breach exposes customer info and government IDs*, BLEEPINGCOMPUTER (May 15, 2025), located at https://www.bleepingcomputer.com/news/security/coinbase-discloses-breach-faces-up-to-400-million-in-losses/ (last accessed on May 30, 2025).

- Whether Defendants failed to properly safeguard the PII of Plaintiff and Class Members;
- Whether Defendants breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;
- Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and
- Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

21. **Typicality.** Plaintiff' claims are typical of the claims of the Class Members. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendants to safeguard their PII. Plaintiff and Class Members entrusted Defendants with their PII, and it was subsequently accessed by an unauthorized third party.

22. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

23. **Superiority.** This class action is appropriate for certification because class

proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

24. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duties and released Plaintiff's and Class Members' PII, then Plaintiff and each Class member suffered damages by that conduct.

25. **Ascertainability:** Members of the Class are ascertainable. Class Membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

FACTUAL BACKGROUND

A. Coinbase Provides Cryptocurreny Exchange Services Involving Highly Sensitive Data

26. Coinbase bills itself as "the most trusted place for people and businesses to buy, sell, and use crypto."[6]

27. Coinbase allows its customers to trade cryptocurrency by providing "a trusted platform that makes it easy for people and institutions to engage with crypto assets, including

[6] *Coinbase*, COINBASE, located at https://www.coinbase.com/ (last accessed on May 30, 2025).

trading, staking, safekeeping, spending, and fast, free global transfers."[7]

28. As part of providing its services, Coinbase is entrusted with its customers' PII. This sensitive PII includes but is not limited to, *inter alia*, names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents).

29. When entrusting Coinbase with their PII, Plaintiff and Class Members reasonably expect Defendants would use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Plaintiff and Class Members had a reasonable expectation, based in part on Coinbase's own statements, that their PII would be protected. Coinbase stated that:

> [t]rust is built on dependable security and protections—which is why we make protecting your account & your digital assets our number one priority. Identity verification is a key part of our regulatory compliance program, and we have built a robust architecture that roots out suspicious users. Our system prioritizes accuracy and adherence to the law across our global regulatory landscape.[8]

31. However, despite Defendants' stated commitment to data security, Coinbase did not adopt reasonable measures to prevent the unauthorized access to Plaintiff's and Class Members' PII by unauthorized bad actors.

---

[7] *About Coinbase*, *supra* note 2.

[8] Gary Shambat, *Identity verification and financial compliance*, COINBASE (March 31, 2023), located at https://www.coinbase.com/blog/identity-verification-and-financial-compliance (last accessed on May 30, 2025).

B. The Data Breach

32. On or about May 11, 2025, Coinbase became aware of a potential cybersecurity incident as Coinbase received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management systems.[9]

33. A threat actor reportedly targeted Coinbase's customer support agents overseas and used cash offers to convince a small group of insiders to copy data in their customer support tools for less than 1% of Coinbase monthly transacting users with the aim of gathering a customer list they could contact while pretending to be Coinbase—tricking people into handing over their cryptocurrency.[10]

34. The threat actor then demanded a $20 million ransom not to publish the stolen information. Defendants said they would not pay the ransom but would establish a $20 million reward fund for any leads that could help find the attackers who coordinated this attack.[11]

35. But even if Defendants took steps to ensure the data's deletion, *i.e.*, paid the threat actors a likely ransom to ensure the stolen information's destruction, criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments, or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

> Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers also threaten to release sensitive stolen data unless the victim

[9] Form 8-K, *supra* note 1.
[10] *Protecting Our Customers - Standing Up to Extortionists*, COINBASE (May 15, 2025), located at https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists (last accessed on May 30, 2025).
[11] Gatlan, *supra* note 5.

> pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.[12]

36. Indeed, Coinbase cannot reasonably maintain the stolen information would be destroyed and will not be further disseminated. Defendants' own notice to impacted individuals advises them to remain vigilant for scammers and take further actions such as enabling heightened security settings.[13]

37. The impacted information includes names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank account numbers and some bank account identifiers, Government ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents).[14]

38. Private assessments of the Data Breach indicate that Coinbase did not implement basic steps to safeguard the PII that it was entrusted. After its own investigation, Coinbase discovered the threat actor gained access to Coinbase's customers' information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems to which they had access in order to perform their job responsibilities.[15]

39. On May 15, 2025, Coinbase reported the Data Breach to its customers that were

---

[12] Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, KREBS ON SECURITY (Nov. 4, 2020), located at https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/ (last accessed on May 30, 2025).
[13] *Protecting Our Customers*, *supra* note 10.
[14] Form 8-K, *supra* note 1.
[15] *Id*.

affected by this incident.[16]

40. Upon information and belief, the Data Breach occurred as a direct and proximate result of Coinbase's intentional, willful, reckless, and/or negligent failure to implement and follow basic security procedures in order to protect its customers' PII. Indeed, had Coinbase properly maintained and monitored its computer systems that stored the PII, Defendants would have discovered the Data Breach sooner rather than allowing the cybercriminals unimpeded access to access and exfiltrate Plaintiff's and Class Members' PII.

41. In any event, the scope of the Data Breach shows the severity of Coinbase's data security failings. The cybercriminals were able to gain access to Coinbase's customers' PII. If Coinbase had even minimal data security measures in place, it would have been able to detect the Data Breach at a point before cybercriminals were able to successfully obtain its customers' data.

C. The Value of PII

42. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[17]

43. In October 2023, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim

[16] *Protecting Our Customers*, *supra* note 10.
[17] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (Apr. 30, 2020), located at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed on May 30, 2025).

data and pressured victims to pay by threatening to release the stolen data."[18]

44. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

45. Malicious actors can use stolen personal information to, *inter alia*, create synthetic identities (which are harder for authorities to detect), execute credible phishing attacks, and sell the personal information on underground markets in the dark web.[19]

46. Another example is when the U.S. Department of Justice announced its seizure of RaidForums in 2022. RaidForums was an online marketplace popular for cybercriminals to purchase and sell hacked data belonging to millions of individuals around the world.[20]

47. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. According to Prey, a company that develops device tracking and recovery software, stolen PII can be worth up to $2,000.00 depending on the type of information obtained.[21]

48. Social Security numbers, for example, are among the worst kind of personal

---

[18] *See StopRansomware Guide*, U.S. CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, located at https://www.cisa.gov/stopransomware/ransomware-guide (last accessed on May 30, 2025).
[19] *What Data Do Cybercriminals Steal? (How To Protect Yours)*, IDENTITY GUARD (Feb. 14, 2024), located at https://www.identityguard.com/news/what-information-do-cyber-criminals-steal (last accessed on May 30, 2025).
[20] *United States Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator*, U.S. DEPT. OF JUSTICE (Apr. 12, 2022), located at https://www.justice.gov/archives/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator (last accessed on May 30, 2025).
[21] Juan Hernandez, *Stolen credentials: their dark web lifecycle and why you can't ignore it*, PREY (Feb. 26, 2024), located at https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web (last accessed on May 30, 2025).

information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. Such fraudulent uses include opening fraudulent credit cards and bank accounts, filing or collecting tax returns, accessing government benefits, applying for loans, and receiving healthcare. "If not spotted and resolved, these types of identity theft can rack up financial debt and do extensive damage to a person's credit, making things like obtaining a loan to buy a car or house difficult or even impossible."[22]

49. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

50. Even then, a new Social Security number may not be effective. "When issuing a new SSN, the Social Security Administration (SSA) links your old number to your new one so you'll still be associated with all wages earned."[23]

51. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than other types of data because the information compromised in this Data Breach is difficult, if not impossible, to change.

52. The PII compromised in the Data Breach also demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security

[22] *What to do if someone has your Social Security number*, ALLSTATE (Jan. 24, 2024), located at https://www.allstateidentityprotection.com/content-hub/stolen-social-security-number (last accessed on May 30, 2025).
[23] Alex Cook, *What Happens if I Change My Social Security Number*, LENDINGTREE (Mar. 15, 2023), located at https://www.lendingtree.com/credit-repair/credit-score-after-getting-a-new-social-security-number/ (last accessed on May 30, 2025).

numbers are worth more than 10x in price on the black market."[24]

53. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

54. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $12.5 billion in losses to individuals and business victims.[25]

55. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

56. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

57. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[26] The GAO Report further notes that this type of identity fraud is the most harmful

---

[24] Tim Greene, *Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers*, NETWORKWORLD (Feb. 6, 2015), located at https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed on May 30, 2025).

[25] *2023 Internet Crime Report*, FED. BUREAU OF INVESTIG. (2023), located at https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf (last accessed on May 30, 2025).

[26] *See* Government Accountability Office, *PERSONAL INFORMATION: Data Breaches are*

because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and] their good name."[27]

58. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

D. Coinbase Failed to Comply with the FTC Act and Failed to Observe Reasonable and Adequate Data Security Measures

59. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[28]

60. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[29]

Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), located at https://www.gao.gov/assets/gao-07-737.pdf (last accessed on May 30, 2025).

[27] *Id*.

[28] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), located at https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf (last accessed on May 30, 2025).

[29] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), located at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed on May 30, 2025).

61. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

62. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[30]

63. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

64. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

65. Plaintiff and Class Members gave their PII to Defendants with the reasonable expectation and understanding that Defendants would comply with their duty to keep such information confidential and secure from unauthorized access.

[30] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), located at https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf. (last accessed on May 30, 2025).

66. Defendants have been on notice for years that Plaintiff's and Class Members' PII was a target for bad actors because of, among other motives, the high value of the PII created, collected, and maintained by Defendants.

67. Despite such awareness, Defendants failed to impose and maintain reasonable and appropriate data security controls to protect Plaintiff's and Class Members' PII from unauthorized access that Defendants should have anticipated and guarded against.

68. Defendants were fully aware of their obligation to protect the PII of its customers because of their collection, storage, and maintenance of PII. Defendants were also aware of the significant consequences that would ensue if they failed to do so because Defendants collected, stored, and maintained sensitive private information from millions of individuals and knew that this information, if hacked, would result in injury to Plaintiff and Class Members.

69. Despite understanding the consequences of insufficient data security, Defendants failed to adequately protect Plaintiff's and Class Members' PII, permitting bad actors to access and misuse it.

E. Defendants Failed to Comply with Industry Standards

70. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[31] All organizations collecting and handling PII, such as Defendants, are strongly encouraged to follow these controls.

[31] *Critical Security Controls*, at 1, CENTER FOR INTERNET SECURITY (May 2021), located at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last accessed on May 30, 2025).

71. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[32]

72. Several best practices have been identified that a minimum should be implemented by entities like Coinbase, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[33]

73. Other best practices have been identified that a minimum should be implemented by entities like Coinbase, including but not limited to ensuring that PII is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.[34]

74. Defendants failed to follow these and other industry standards to adequately protect the PII of Plaintiff and Class Members.

F. The Data Breach Caused Harm and Will Result in Additional Fraud

75. The ramifications of Defendants' failure to secure Plaintiff's and Class Members' data are severe.

76. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of

[32] *See CIS Benchmarks FAQ*, CENTER FOR INTERNET SECURITY, located at https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last accessed on May 30, 2025).
[33] *See Critical Security Controls*, CENTER FOR INTERNET SECURITY (May 2021), located at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last accessed on May 30, 2025).
[34] *See id*.

data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

77. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[36]

78. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

79. As demonstrated herein, these and other instances of fraudulent misuse of the compromised PII has already occurred and are likely to continue.

80. Javelin Strategy and Research reports that identity thieves stole $43 billion in 2022.[37]

81. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. According to Experian, a credit monitoring

[35] 17 C.F.R § 248.201 (2013).
[36] *Id*.
[37] *See Identity Fraud Losses Totaled $43 Billion in 2022, Affecting 40 Million U.S. Adults*, JAVELIN (Mar. 28, 2023), located at https://javelinstrategy.com/press-release/identity-fraud-losses-totaled-43-billion-2022-affecting-40-million-us-adults (last accessed on May 30, 2025).

company, "[a]lthough 28% [of identity theft victims] said they resolved their issues within six months of an ID theft incident, 65% said issues remained unresolved even after a year."[38]

82. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

83. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

G. Plaintiff's Experience

84. Plaintiff is a customer of Coinbase and exchanges cryptocurrency on its platform. In order to utilize Defendants' exchange, Plaintiff had to entrust Coinbase with his PII. In collecting and maintaining the PII of Plaintiff, Defendants undertook a duty to act reasonably in their handling of Plaintiff's PII. Coinbase, however, did not take reasonable care of Plaintiff's PII, leading to its exposure and compromise as a direct result of Defendants' improper data security measures.

85. Plaintiff has started receiving spam calls and texts relating to his Coinbase account.

86. Since the announcement of the Data Breach, Plaintiff has had to spend his valuable

---

[38] Gayle Soto, *What Are the Unexpected Costs of Identity Theft*, EXPERIAN (July 30, 2024), located at https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/ (last accessed on May 30, 2025).

[39] *See* Government Accountability Office, *PERSONAL INFORMATION: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), located at https://www.gao.gov/assets/gao-07-737.pdf (last accessed on May 30, 2025).

time and effort taking steps to avoid potential scams attempting to gain access to his account and mitigate the risk of misuse of his PII. Specifically, Plaintiff has had to spend his valuable time and effort monitoring his Coinbase account and resetting passwords to his financial accounts. Plaintiff would not have had to engage in these time intensive efforts but for the Data Breach.

87. Plaintiff has suffered actual injury from having his PII exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent scammers accessing his account; (b) mitigation efforts to prevent the misuse of his PII; (c) damages to and diminution of the value of his PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (d) loss of privacy.

88. Given the nature of the information compromised in the Data Breach and the propensity of criminals to use such information to commit a wide variety of crimes, Plaintiff faces a significant, present, and ongoing risk of scams, identity theft and fraud, and other identity-related fraud now and into the indefinite future.

89. In addition, knowing that hackers gained access to his PII and that this information likely has been and will be used in the future for scams, identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

H. Plaintiff and Class Members Suffered Damages

90. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class

Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

91. Had Defendants remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented intrusion into its information storage and security systems and, ultimately, the theft of the PII of over one million individuals.

92. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their PII, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

93. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the improper disclosure of their PII;

d. loss of privacy;

e. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and,

g. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

94. While Plaintiff's and Class Members' PII has been stolen, Defendants continue to hold Plaintiff's and Class Members' PII. Particularly because Defendants have demonstrated an inability to prevent a breach, Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLAIMS FOR RELEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

95. Plaintiff restates and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

96. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

97. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class Members' PII in Defendants' possession was properly secured and protected; (b) implementing processes that would detect a breach of their security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

98. Coinbase's duty to use reasonable care arose from several sources, including but not limited to those described below.

99. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any improper security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Coinbase was obligated to act with reasonable care to protect against these foreseeable threats.

100. Defendants also owed a common law duty because their conduct created a

foreseeable risk of harm to Plaintiff and Class Members. Coinbase's conduct included its failure to properly restrict access to its computer networks and/or servers that held individuals' PII.

101. Defendants also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing appropriate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach in the financial sector.

102. Defendants breached the duties owed to Plaintiff and Class Members and thus was negligent. Coinbase breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to properly test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies provided to customers; and (h) failing to properly train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

103. But for Coinbase's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been access, exfiltrated, and compromised by cybercriminals.

104. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries including:

a. Theft of their PII;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted to Coinbase with the mutual understanding that Defendants would safeguard Plaintiff' and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and proper measures to protect Plaintiff and Class Members.

105. As a direct and proximate result of Coinbase's negligence, including its gross negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

106. Plaintiff restates and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

107. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Coinbase for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duties.

108. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect customers' PII and not complying with the industry standards. Coinbase's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

109. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

110. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

111. Coinbase's violation of Section 5 of the FTC Act constitutes negligence *per se*.

112. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 99 above.

113. As a direct and proximate result of Coinbase's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including

compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

114. Plaintiff restates and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

115. Plaintiff and Class Members conferred a monetary benefit on Coinbase by providing them with their valuable PII.

116. Coinbase knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiff's and Class Members' PII and use of Plaintiff's and Class Members' PII for business purposes.

117. Defendants did not secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

118. Coinbase acquired the PII through inequitable record retention as it did not disclose the improper data security practices previously alleged.

119. If Plaintiff and Class Members had known Defendants would not use appropriate data security practices, procedures, and protocols to properly monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Defendants.

120. Under the circumstances, it would be unjust for Coinbase to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

121. Plaintiff and Class Members are without an adequate remedy at law.

122. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 98 above.

123. Plaintiff and Class Members are entitled to restitution and/or damages from Coinbase and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

124. Plaintiff restates and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

125. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

126. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Coinbase is currently maintaining data security measures appropriate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendants still possess Plaintiff's and Class Members' PII, and that Defendants' data security measures remain improper. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

127. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

j. Defendants owe a legal duty to secure consumers' PII under the common law

and Section 5 of the FTC Act; and

k. Defendants continue to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' PII.

128. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ appropriate security protocols consistent with law and industry standards to protect consumers' PII in their possession.

129. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Coinbase. The risk of another such breach is real, immediate, and substantial. If another breach at Coinbase occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

130. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

131. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays

for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff' reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 26, 2025

GLANCY PRONGAY & MURRAY LLP

By: */s/ Brian P. Murray*

Brian P. Murray (BM 9954)
230 Park Avenue, Suite 358
New York, NY 10169
Tel: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

LAW OFFICE OF PAUL C. WHALEN
Paul C. Whalen
768 Plandome Road
Manhasset, NY 11030
Tel: (516) 426-6870
pcwhalen@gmail.com

Attorneys for Plaintiff and the Proposed Class